脆弱性検査結果の推移について

情報政策課　技術専門職員　金森　浩治

1．はじめに

富山大学では2014年からNessusによる脆弱性検査を実施している。前稿ではその実施と運用について述べた。[1]

本稿では過去4回分の脆弱性検査結果の推移について述べる。

2. Nessusとは

Nessusとは，ネットワーク経由でターゲットホストの脆弱性，設定，マルウエアプロセスを含む様々な情報を収集しシステムの脆弱性をスキャンするソフトウェアである。Windows, Linux, Macなど様々なプラットフォームに対応しており，スキャンできる対象も様々なOS, ネットワーク機器, 仮想環境プラットフォーム，データベース Webアプリケーション，クラウドサービス，モバイルデバイスなど幅広く対応している。[2]

なおNessusではXSSやSQLインジェクションといったアプリケーション層に起因する脆弱性を検出することはできない。

3. 運用について

Nessusによる脆弱性スキャンは2014年度から年一回ペースで計4回行っている。

検査・分析・通知・改修/報告といった基本的な運用手順については昨年度の富山大学総合情報基盤センター広報（vol.14）で述べた通りである。

4. 各年度の検査・改修/報告結果の推移について

各年度の脆弱性検査結果の推移を図1に示す。

縦軸に台数（IPアドレス数），横軸に年度，リスクがCriticalのものを青線，Highのものを赤線で示している。

2014年度と2015年度のHigh件数に大きな変化がないのは，2014年度は初年度ということもあり，作業量が予測つかなかったため。Criticalのみエンドユーザに通知したためである。

また，2016年度のCritical件数が増えているのは，端末室に使用している同一パソコンやネットワーク機器にCriticalの脆弱性が見つかったためである。

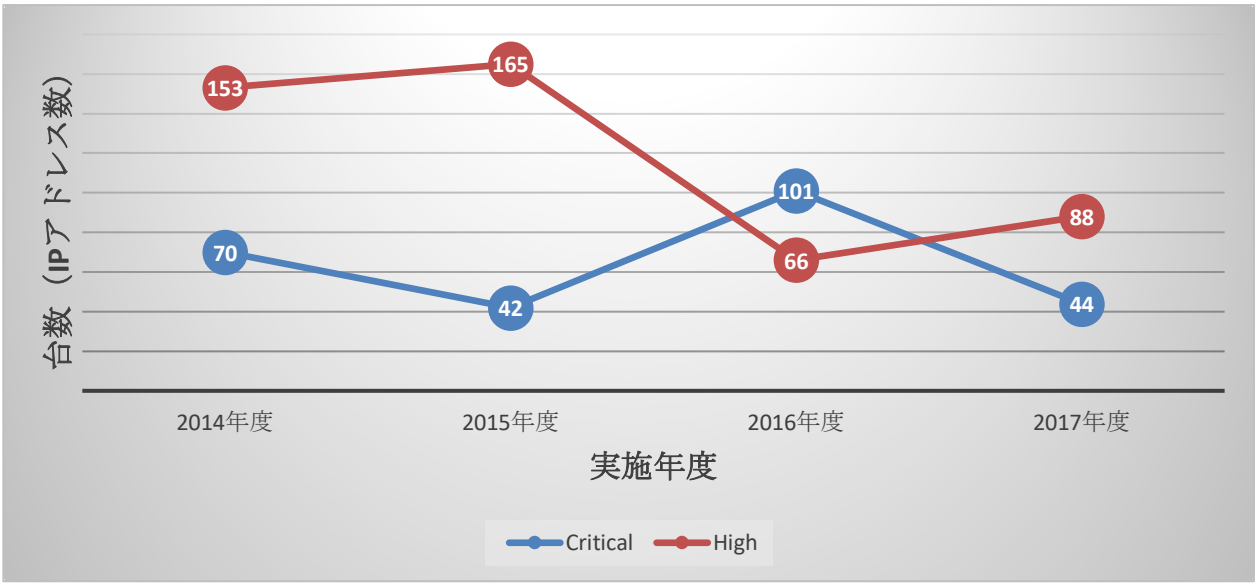

図 1　脆弱性検査結果（台数）

続いて，縦軸に機器管理者数（人），横軸に年度，リスクが Critical のものを青線，High のものを赤線で示したものを図 2 に示す。

これを見ると Critical，High 共に右肩下がりの傾向を示していることから、本学において脆弱性検査がある一定の効果があらわれていることがわかる。

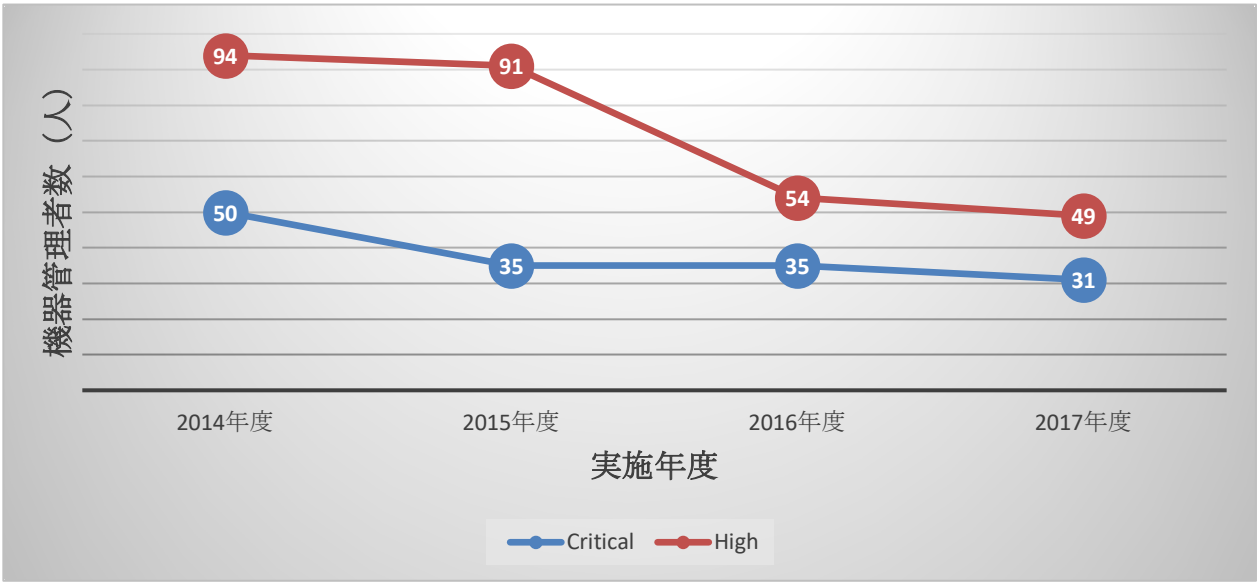

図 2　脆弱性検査結果（機器管理者数）

最後に，過去 3 回以上 Critical もしくは High の脆弱性が検出された IP アドレスの機器種別結果を以下に示す。

[4 回検出された機器]

・プリンター	1 台
・NAS	3 台
・無線 LAN 機器	1 台
・PC サーバー	1 台

[3 回検出された機器]

・プリンター	14 台
・NAS	5 台
・無線 LAN 機器	3 台
・PC サーバー	2 台
・不明	2 台

そもそも Nessus よる脆弱性検査は夜通し行っているためサーバー機能を持つ機器の脆弱性を検出しやすい傾向にあり，また IoT 機器については脆弱性に対応したファームウェアが提供されていなかったり脆弱性を生んでいるサービス(デーモン)を停止できなかったりするため，十分な対応が出来ず，その結果このような結果になっていると想定される。

参考文献

[1] Nessus による脆弱性スキャンの実施と運用について（富山大学総合情報基盤センター広報，vol.14,33-34）

[2] 脆弱性スキャナー Nessus 利用ガイド初級編（http://www.slideshare.net/RyuichiTomita/nessus-start-guidejprev1）